IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

IN THE MATTER OF THE SEARCH OF: THE PRODUCTION OF "diplomatsblessing@icloud.com AND diplomatsblessing@gmail.com" DOWNLOADED FROM APPLE INC. IN THE POSSESSION OF THE FBI	Case No. 1:24-mj-698 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Randy Larkin, Affiant, being duly sworn under oath deposes and states:

INTRODUCTION AND AGENT BACKFGROUND

I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at the FBI Resident Agency located in Williston, North Dakota, which were previously downloaded pursuant to a search warrant from premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. Your affiant requests an additional search warrant to search the diplomatsblessing@icloud.com AND diplomatsblessing@gmail.com accounts downloaded from Apple for Child Sexual Abuse Material (CSAM) because your affiant located CSAM during a search of the information provided by Apple, as noted in paragraph 30 below.

The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(l)(A) to require Apple Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

1. I am a Special Agent with the FBI and have been since September 2015. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am currently assigned to the Minneapolis Division, Williston, North Dakota Resident Agency, of the FBI. I am tasked with investigating a number of criminal offenses including the investigation of drug trafficking organizations, public corruption, financial crime, and violent crime and assault within boundaries of Native American Indian Reservations. Since becoming a Special Agent, I have participated in investigations involving drug trafficking, criminal cyber, national security cyber, financial crimes, international terrorism, and violent crimes against children. I have conducted or participated in physical and electronic surveillance, the execution of search warrants, arrests, and utilizing informants for controlled narcotics purchases. I hold a master's degree in Information Security and Computer Technology. Through my training, education, and experience, I have become familiar with email communications. Since September 2023 I have been a member of the FBI Cellular Analysis Survey Team (CAST).
2. On 10/22/2024, this court granted a search warrant for review of the iCloud account data produced by Apple, pursuant to Eighth Circuit Court of Appeals case entitled *United States v. Nyah*, 928 F.3d 694 (8th Cir. 2019). On or about 11/1/2024, FBI SA Randy Larkin was reviewing the Apple iCloud production for the accounts diplomatsblessing@icloud.com and diplomatsblessing@gmail.com which approximated over 100GB worth of photos, videos, and documents. During the

review, SA Larkin encountered a video of approximately 2:30 in length that depicted CSAM. SA Larkin stopped the review. This warrant is to add the additional federal statute to investigate violations of 18 U.S.C. Section 2252 and 2252A (Certain activities relating to material involving the sexual exploitation of minors).

As a Special Agent with the FBI, I have authority to investigate violations of federal law. I also have authority to seek and execute federal process, to include search warrants. I make this affidavit in support of a search warrant in connection to the offenses of Title 18, United States Code Sections 1341, 1343, 1349, and 2, mail fraud, wire fraud, conspiracy to commit mail and wire fraud, and aiding and abetting mail and wire fraud. As well as Title 18 United States Code Sections 2252 and 2252A (Certain activities relating to material involving the sexual exploitation of minors).

3. Based on my training, experience, and the facts set forth in this affidavit, I believe there is probable cause to believe that the user of the accounts listed below, committed the violation of: Title 18, United States Code Sections 1341, 1343, 1349, and 2, mail fraud, wire fraud, conspiracy to commit mail and wire fraud, and aiding and abetting mail and wire fraud. There is also probable cause that the user of the accounts committed the violation of: Title 18, United States Code Sections 2252 and 2252A (Certain activities relating to material involving the sexual exploitation of minors). Specifically, there is probable cause demonstrating that this individual is involved in a scheme to defraud pertaining to romance scams and is in an organizer or leader role based outside of the United States. There is probable cause demonstrating that the user is in possession of CSAM. I believe there is probable cause to search the information

described in Attachment A for evidence of these crimes further described in Attachment B.

a) diplomatsblessing@gmail.com **(DSID 8197905611);**

b) diplomatsblessing@icloud.com **(DSID 10197364090);**

There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

4. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is a district court of the United States that has jurisdiction over the offense(s) being investigated.

PROBABLE CAUSE

Background of North Dakota Victims

5. The targets of this investigation, JULIET MOLENDA, CHINEDU NWAFOR, and VITUS UZOWURU, have participated in a romance scam since at least January 2020, in which the scheme participants induce their victims to send money to other co-conspirators based on false claims. The suspects find their victims online, typically through dating websites or social media websites or applications. The suspects create fake profiles, including photos of other people (i.e., unsuspecting third parties not connected to the fraud) to attract victims who are seeking companionship and intimate relationships. The suspects begin communicating with the victims and, over a period of time, cultivate these victims' trust. Usually, the co-conspirators concoct elaborate stories to convince victims to provide them with money. Typically, a co-conspirator will tell a victim that the fake object of his or her affection is stuck overseas, unable to leave without paying costs or fees associated with a work project gone awry, a sudden legal issue, or a customs dispute. In such cases, a network of co-conspirators involved in the fraud

will pose as different agents of the fake love interest (such as attorneys or diplomats) who are supposedly working to move funds needed by the fake love interest.

6. Victim M.H. is 79 years old and lives in Tigoa, North Dakota. Victim M.H. was the target of a romance and elder fraud scam. Victim M.H. maintained a bank account with Bank of Tioga, located in Tioga, North Dakota. In August 2022, Victim met a man on Facebook purporting to be an individual named CHRISTOPHER J. MAHONEY who claimed he was a United States Marine stationed in Syria. Between August 2022 and January 2023, Victim M.H. communicated with the person purporting to be MAHONEY through both Facebook Messenger and Google Hangouts and had conversations of a romantic nature with MAHONEY. Victim M.H. sent approximately $800,000.00 to individuals at the direction of MAHONEY or at the direction of individuals to whom MAHONEY introduced Victim. Victim M.H. initiated two formal wire transfer requests at the Bank of Tioga to send two separate $50,000.00 wire transfers, totaling $100,000.00, from victim's Bank of Tioga account, located in Tioga, North Dakota, to a Navy Federal Credit Union account, located in Cheltenham, Maryland, and associated with JULIET MOLENDA. Ultimately, due to suspecting fraud, Bank of Tioga declined sending these two $50,000.00 wire transfers to JULIET MOLENDA's Navy Federal Credit Union account. However, as noted in paragraphs 14 through 19, *infra*, and as alleged in an indictment charging JULIET MOLENDA with wire fraud and aiding and abetting wire fraud, two additional known romance scam victims, D.F and M.T., successfully sent money to JULIET MOLENDA's Navy Federal Credit Union account.

7. On 4/12/2023, a grand jury in the United States District Court for the District of North Dakota returned an indictment charging JULIET CHINYERE MOLENDA, a/k/a Juliet Kingsley,

with the following violations of federal law: 18 U.S.C. 1343 (Wire Fraud), and 18 U.S.C. 1349 (Aiding and Abetting) and a Forfeiture Allegation.

8. On 5/10/2023, MOLENDA was arrested at her residence located at 9716 Spinnaker St, Cheltenham, MD. After the arrest, MOLENDA was transported to the United States District Court in Greenbelt, MD by USPIS Postal Inspector Nichole Rodriguez and FBI SA Randy Larkin. After being read her Miranda rights by SA Larkin, MOLENDA explained to the transporting agents that she worked as a food delivery driver and that she made organic fruit drinks for people. MOLENDA also mentioned that she sold cars.

PO Boxes Associated With Targets

9. After MOLENDA's arrest, SA Larkin learned from Inspector Rodriguez that MOLENDA was working with CHINEDU NWAFOR and VITUS UZOWURU and that there were multiple USPS PO Boxes that were opened and shared between the three individuals. Further, there were multiple different confirmed romance scam victims, all of whom had sent money via cash or cashier's check to the PO Boxes controlled by NWAFOR, MOLENDA, and UZOWURU. Additionally, some of the victims named in the MOLENDA indictment sent money directly to MOLENDA's J-Will Global LLC Navy Federal Credit Union account and sent money to PO Boxes controlled by NWAFOR and MOLENDA. Specifically, victim D.F. from Mukwonago, WI sent money to both MOLENDA's J-Will Global LLC Navy Federal Credit Union account and the PO Box associated with MaryJuls Investment, LLC, owned by NWAFOR. Victim M.T. from Columbia Station, OH, sent money to MOLENDA's J-Will Global LLC Navy Federal Credit Union account and to PO Box 31241, a PO Box controlled by MOLENDA. Both M.T. and D.F. believed that they were communicating with General ANDREW GLENN GODDARD.

10. CHINEDU NWAFOR, VITUS UZOWURU**,** and JULIET MOLENDA have opened and controlled multiple United States Postal Service (USPS) PO Boxes in Maryland and Washington, DC to receive funds from victims of romance scams.

11. According to USPS records, CHINEDU NWAFOR, VITUS UZOWURU, and JULIET MOLENDA opened and/or were authorized recipients of numerous PO Boxes listed below. SA Larkin knows that the opening of multiple PO Boxes in a short period of time at various Post Offices is not consistent with normal business or personal usage of PO Boxes.

Date Opened	**PO Box #**	**City**	**State**	**Applicant Business name / Individual**	**Authorized Recipients**
1/21/2020	154	Cheltenham	MD	Chinedu **NWAFOR**	CN, Juliet **MOLENDA**, JCM, Vitus **UZOWURU**
5/18/2020	5705	Capitol Heights	MD	Chinedu **NWAFOR**	CN, Vitus **UZOWURU,** Vage Global Resources LLC
4/28/2021	939	Clinton	MD	"CN", Chinedu **NWAFOR**	N/A
5/6/2021	509	Brandywine	MD	"JM", Juliet **MOLENDA**	N/A
9/9/2021	41068	Washington	DC	Chinedu **NWAFOR**	NC, Vitus **UZOWURU**
9/10/2021	6748	Upper Marlboro	MD	Chinedu **NWAFOR**	N/A
9/23/2021	2337	Waldorf	MD	JJOscar Motors LLC, Juliet **MOLENDA**	N/A
11/4/2021	41460	Washington	DC	Chinedu **NWAFOR**	N/A
2/14/2022	2737	Landover Hills	MD	Maryjuls Investments LLC, Chinedu **NWAFOR**	N/A
8/8/2022	31241	Washington	DC	Juliet **MOLENDA**	N/A

Additional Victims

12. Victim V.J.B. is 77 years old and lives in New Town, ND. Victim V.J.B. was the target of a romance fraud scam and matches the profile of an elderly female. VJ.B. is suspected

of mailing at least three parcels containing money or checks to known fraudulent PO Boxes in MD. Parcel with USPS tracking number EJ303734865US was mailed on November 20, 2021, from New Town, ND to PO Box 154, Cheltenham, MD 20623, which is the PO Box associated with MOLENDA, NWAFOR, and UZOWURU. Parcel with USPS tracking number EJ839780587US was mailed on December 21, 2021, from Watford City, ND to PO Box 154, Cheltenham, MD 20623. Parcel with USPS tracking number EJ235566043US was mailed on April 7, 2022, from New Town, ND to PO Box 2737, Hyattsville, MD 20784, which is the PO Box associated with NWAFOR.

13. According to USPS records, on or about January 21, 2020, PO Box 154, Cheltenham, MD 20623, was registered to NWAFOR CHINEDU, address 9716 Spinnaker Street, Cheltenham, MD 20623. The email listed on the application was Dumebi136@gmail.com. The application listed additional names of individuals authorized to receive mail at the PO Box including "CN," JULIET MOLENDA, "JCM," and VITUS UZOWURU.

14. Victim D.F. is 72 years old and lives in Mukwonago, WI. Victim D.F. was the target of a romance scam and advance fee scam. Navy Federal Credit Union records from JULIET MOLENDA's Navy Federal Credit Union accounts demonstrate that Navy Federal Credit Union accounts ending in 3541 and 2548 received the following checks from D.F., as noted below:

- September 8, 2022: An Associated Bank cashier's check written from D.F. to J-Will Global LLC in the amount of $30,000.00 (account ending in 2548);
- September 12, 2022: An Associated Bank cashier's check written from D.F. to J-Will Global LLC in the amount of $30,000.00 (account ending in 3541); and
- September 30, 2022: An Associated Bank cashier's check written from D.F. to

J-Will Global LLC in the amount of $10,000.00 (account ending in 3541).

WIRE to Paul Miller Auto Group, LLC, Parsippany NJ

15. Victim D.F. was interviewed by SA Larkin. Victim D.F. explained that she was communicating with an individual purporting to be a United States military general named ANDREW GLENN GODDARD. The purpose of the cashier's checks was to pay the diplomat to release the portfolio and help GODDARD return home from Syria. On or about 8/19/2022, D.F. sent a $30,000 cashier's check made payable to MaryJuls Investment LLC to address PO Box 2737, Hyattsville, MD 20784. This was the same PO Box where possible victim V.J.B. also sent a parcel on or about 4/7/2022.

16. According to USPS records, on or about February 14, 2022, PO Box 2737, Hyattsville, MD 20784 was registered to Maryjuls Investments LLC by CHINEDU NWAFOR. The PO Box application indicated the box was for business use. The email listed on the application was Dumebi136@gmail.com.

17. According to Maryland Department of Assessments & Taxation (MDDAT), Maryjuls Investments LLC, 16701 Melford Blvd, Suite 400, Bowie, MD 20715, was registered on or about October 6, 2021. CHINEDU NWAFOR is listed as an authorized person on the articles of organization.

18. Victim M.T. is 65 years old and lives in Columbia Station, Ohio. Victim M.T. was the target of a romance and advance fee scam. Navy Federal Credit Union records from JULIET MOLENDA's Navy Federal Credit Union accounts demonstrate that Navy Federal Credit account ending in 3541 received the following check from M.T., as noted below:

- December 9, 2022: a Fifth Third Bank cashier's check written from M.T. to J/Will Global LLC in the amount of $45,000.00.

19. SA Larkin interviewed Victim M.T. Victim M.T. explained that she was communicating with an individual purporting to be a United States military general named ANDREW GLENN GODDARD. Victim M.T. confirmed that the money was for the general's "portfolio." Victim M.T. also provided a picture of a package that she sent to the address, JCM, P.O. Box 31241, Washington, DC 20030. This PO Box is listed in the above table as being associated with JULIET MOLENDA.

Additional Subject Identified

20. On September 27, 2023, a federal grand jury in the District of North Dakota returned an indictment charging NWAFOR and UZOWURU with mail fraud and conspiracy to commit mail fraud. On October 11, 2023, NWAFOR was arrested and NWAFOR's phone was seized by law enforcement. SA Larkin obtained a search warrant for NWAFOR's phone and reviewed the contents of the phone. During review of the phone there were approximately 175 photos of USPS package labels with mostly female names. There were also numerous chat messages with references to, "dating jobs," and splitting money amongst individuals which indicate that NWAFOR was part of the romance scam mail fraud conspiracy.

21. Additionally, based upon a review of communications found within NWAFOR's phone, NWAFOR was communicating with an individual on Telegram and WhatsApp with the display name, "King Roy." NWAFOR sent King Roy three videos around July 19, 2023, where he, NWAFOR, was sitting in a car reading out USPS label confirmation numbers, opening packages, and counting cash that was contained within the packages. NWAFOR was sending these videos to King Roy. The two phone numbers in NWAFOR's phone for King Roy were, +905362292730 and +905525873066.

22. On August 8, 2024, this Court issued a judgement sentencing UZOWURU on a single count of Aiding and Abetting Mail Fraud.

23. On September 12, 2024, NWAFOR pleaded guilty to a single count of Conspiracy to Commit Mail Fraud.

24. On 7/30/2024, COOPERATING WITNESS was interviewed pursuant to a proffer session. According to COOPERATING WITNESS, the person that told COOPERATING WITNESS to open up all of the USPS P.O. boxes and accept money and packages was, OBIORA ANISUDE a/k/a KING ROY, hereafter ANISUDE. COOPERATING WITNESS knew ANISUDE from when he was living in Istanbul, Turkey. In 2021, when COOPERATING WITNESS was approached by law enforcement at the post office, he left and called ANISUDE to ask what was going on. ANISUDE said he would, "call them," indicating his counterparts in Nigeria that were chatting to romance scam victims. ANISUDE told COOPERATING WITNESS that he, ANISUDE, posed as a diplomat to get money. COOPERATING WITNESS would receive money and then take approximately 10 percent to keep for himself and send ANISUDE the rest of the money. COOPERATING WITNESS estimated that he sent ANISUDE approximately $400,000 to $500,000 but some weeks or months COOPERATING WITNESS would not have any money to send to ANISUDE.

25. A review of the email account, jckingsley25@gmail.com, the account belonging to MOLENDA, found that on or about 9/14/2022, MOLENDA sent 2,400,000 NGN to OBIORA ANISUDE. There was an email confirmation of this transaction in MOLENDA's account. Open source research showed that 2,400,000 NGN was equivalent to $1,509.33 USD.

Apple iCloud Accounts diplomatsblessing@gmail.com (DSID 8197905611) and diplomatsblessing@icloud.com (DSID 10197364090)

26. On or about 8/26/2024, FBI SA Randy Larkin received a subpoena response from Apple Inc for phone numbers purported to be associated with ANISUDE. The Apple response showed that phone number +905525873066 was associated with Apple person ID 8197905611, with the email diplomatsblessing@gmail.com, name "King Roy", address Coruh Sk. 11A, 34363 Istanbul, Şişli, and billing first and last name OBIORA ANISUDE.

27. By way of background, Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Apple also provided that the DSID corresponds to a unique numeric identifier for an Apple ID.

28. The same subpoena return also provided information on Apple DSID 10197364090, with the name diplomatsblessing@icloud.com. The name associated with the account was, "Steve Okoh", address Sisli, Istanbul, Turkey 30050. The billing full name was listed as, "David Tuoyo Okoh." The telephone number listed for the day phone was, +905394489357. The two verified telephone numbers associated with the account were listed as, +905362292730 and +905525873066. Note, the reason this additional DSID was provided from the subpoena return was because of the verified phone number ending in 3066 which was consistent with OBIORA ANISUDE, indicating this is a second account and/or phone used by ANISUDE.

29. Based on the information above, it is reasonable to believe that the individual using the icloud accounts diplomatsblessing@gmail.com (DSID 8197905611) and diplomatsblessing@icloud.com (DSID 10197364090) are being used by ANISUDE, who is involved in fraud. Specifically, the phone numbers consistent with country code of Turkey as

well as the use of the likely fictious name, "Steve", which is consistent with MOLENDA's statements that a person named, "Mr. Steve" was communicating with her and instructing her to accept fraudulent money.

30. On 9/16/2024, this Court issued a search warrant to Apple Inc. for information associated with the iCloud accounts detailed above. The responsive materials were not produced by Apple until on or about 10/20/2024. On or about 10/21/2024, SA Larkin downloaded the responsive materials from Apple. SA Larkin did not review the content of any of the files. As a result, the response to the search warrant issued on 9/16/2024 was not provided by Apple within the fourteen (14) period provided by Rule 41 Federal Rules of Criminal Procedure. Pursuant to Eighth Circuit Court of Appeals case entitled *United States v. Nyah*, 928 F.3d 694 (8th Cir. 2019), therefore SA Larkin obtained an additional warrant on or about 10/22/2024 to search the production from Apple.

On or about 11/1/2024, SA Larkin was reviewing the Apple iCloud production for the accounts diplomatsblessing@icloud.com and diplomatsblessing@gmail.com which approximated over 100GB worth of photos, videos, and documents. During the review, SA Larkin located a video of approximately 2:30 in length that depicted Child Sexual Abuse Material (CSAM).

Specifically, the video depicted a young, African American boy, approximate age 4-5 years old who was naked and being fondled by a naked African American girl, approximate age 13-15. The girl then bent over and attempted to instruct the boy to penetrate her. The girl stood up and instructed the boy to perform oral sex on her. The girl wiped the boy's mouth and penis with water and then began performing oral sex on the boy. The act was taking place outdoors in a structure resembling a wooden shed or hut with dirt flooring and laundry hanging off the

structure. After review of this video, SA Larkin temporarily discontinued the review until an additional search warrant could be obtained.

BACKGROUND CONCERNING APPLE[1]

31. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

32. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or

Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

33. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

34. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

35. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

36. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including

communications regarding a particular Apple device or service, and the repair history for a device.

37. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

38. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

39. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and

experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

40. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

41. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

42. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages,

Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

43. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

Based on the forgoing, I request that the Court issue the proposed search warrant to search the diplomatsblessing@icloud.com AND diplomatsblessing@gmail.com accounts downloaded from Apple for Child Sexual Abuse Material (CSAM) because, as noted in paragraph 30 above, your affiant located CSAM during a search of the information provided by Apple. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

Randy M. Larkin
Special Agent, Federal Bureau of Investigation

Sworn and subscribed before me on Nov 4, 2024

CLARE R. HOCHHALTER
UNITED STATES MAGISTRATE JUDGE